Department of Homeland Security Daily Open Source Infrastructure Report for 5 March 2008

Current Nationwide

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here

- According to the Associated Press, a Union Pacific train has derailed in the Southern California desert town of Mecca, setting two tanker cars ablaze. One tanker car was carrying phosphoric acid, and another was carrying hydrochloric acid. Riverside County Fire captain said a one-mile radius has been set up around the accident site and no one is being let inside because of the potentially hazardous fumes. (See item **5**)
- The Los Angles Times reports China in the last year has developed ways to infiltrate and manipulate computer networks around the world in what U.S. defense officials conclude is a new and potentially dangerous military capability. Computer network intrusions at the Pentagon and other U.S. agencies, think tanks, and government contractors last year "appeared to originate" in China, according to the report. (See item **34**)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) – [http://www.esisac.com]

1. *March 4, Christian Science Monitor* – (National) **U.S. coal power boom suddenly wanes.** Concerns about global warming and rising building costs are blocking construction of new coal-fired power plants in the U.S. and pushing utilities to turn to natural gas and renewable power instead. Utilities canceled or put on hold at least 45 coal plants in development last year, according to a new analysis by the U.S.

Department of Energy’s National Energy Technology Laboratory. These moves – a sharp reversal from a year ago, when the industry had more than 150 such plants in development – signal the waning of a major U.S. expansion into coal. Natural-gas and renewable power projects have leapt ahead of coal in the development pipeline, according to Global Energy Decisions. Gas and renewables each show more than 70,000 megawatts under development compared with about 66,000 megawatts in the coal-power pipeline. Some call the growing resistance to coal power worrying. “There’s a serious crunch with respect to having enough generating capacity coming in the next ten years,” said the chief executive officer of North American Electric Reliability Corp. “If coal doesn’t play its role, it’s going to be a major issue.” An activist with the Sierra Club said, “There’s not going to be a big need for more coal. There are plenty of alternatives coming.”
Source:
http://news.yahoo.com/s/csm/20080304/ts_csm/acoalcuts;_ylt=AsiErt0CSycAmhKgjR2fnGAPLBIF

2. *March 4, RenewableEnergyWorld.com* – (International) **Technology advancements allow batteries to store more wind energy.** The gigantic wind turbines in Donegal on the west coast of Ireland are on the cutting edge of a revolutionary technology for storing large amounts of energy from wind power. The 32-megawatt wind park in Sorne Hill will be the first in Europe to integrate a big back-up battery system that will ensure a reliable supply of electricity no matter how big the fluctuations in the wind might be. “The battery enables large amounts of energy from wind or solar power to be stored, managed, controlled, and sent into the electricity grid when it is needed. It doesn’t matter whether the wind is blowing or not, the battery makes the electricity output predictable and reliable,” said the CEO of VRB Power Systems, the Canadian manufacturers of the battery. The battery soaks up electricity when the wind turbines produce an excess amount for the system. It then feeds the electricity into the system almost instantaneously as soon as the wind speed drops. It can make electricity from wind 95 percent constant. The VRB battery can be deep-cycled 14,000 times, much more than a conventional lead-acid battery. It is also greener than other batteries and made without toxic metals such as lead, cadmium, zinc, and nickel.
   Source:
   http://www.renewableenergyworld.com/rea/news/story;jsessionid=CB25EBE9F6E3FCD526BF83E48583CFFC?id=51729

3. *March 4, Miami Herald* – (Florida) **Users may be able to sell power to FPL.** In a move that could dramatically expand renewable energy in Florida, state regulators are expected on Tuesday to approve a rule that will require utilities to pay homeowners and businesses for the extra energy they produce from solar panels on their property. The concept, called ‘‘net metering,’’ comes before the Public Service Commission for final approval after a year of discussions. The state already has a net-metering rule for homeowners, but it is hardly ever used, said a director at the Florida Solar Energy Center. Only about 200 customers statewide now participate in the program. Under the current rule, participants get back only three or four cents per kilowatt/hour for the power they provide, far less than the 11 or 12 cents per kw/h they pay as the retail price.

Under the proposed change, energy providers would get credit at the same retail rate that they have to pay. Moreover, while the old rule limits service to homeowners and small businesses, the new rule will allow major corporations to set up huge fields of panels on their large roofs to produce up to two megawatts of power. In addition, the current rule applies only to solar; the change would apply to all renewable energy. The state's utilities support net-metering, but are pushing for requirements for even the smaller customers to pay for circuit breakers to protect their solar systems from the grid in case of a problem.
Source: http://www.miamiherald.com/103/story/442919.html

[Return to top]

Chemical Industry Sector

4. *March 4, University of Arizona* – (National) **US cities at high risk for terrorist attacks identified.** A University of Arizona researcher has created a new system to dramatically show American cities their relative level of vulnerability to bioterrorism. The expert on environmental risk has placed 132 major cities -- from Albany, New York, to Youngstown, Ohio -- on a color-coded map that identifies their level of risk based on factors including critical industries, ports, railroads, population, natural environment and other factors. The map marks high-risk areas as red, midrange risk as yellow and lower risk as green. The map also shows a wide swath of highest-risk urban areas running from New York down through the Southeast and into Texas. Boise is the only high-risk urban area that lies outside the swath. The model employs what risk experts call a benchmark vulnerability metric, which shows risk managers each city's level of risk for urban terrorism. The researcher says terrorism vulnerability involves three dimensions of risk -- social aspects, natural hazards and construction of the city and its infrastructure. He concludes that the allocation of funds for preparedness and response to terrorism should take into account these factors of vulnerability. The research, funded by the U.S. Department of Homeland Security, was published in a recent issue of Risk Analysis, a journal published by the Society for Risk Analysis.
   Source: http://www.sciencedaily.com/releases/2008/03/080304092842.htm

5. *March 4, Associated Press* – (California) **Train derails; acid tanker cars burn.** A Union Pacific train derailed in the Southern California desert town of Mecca, setting two tanker cars ablaze. The accident happened around 9:30 p.m. Monday. Fire officials said about 60 residents in nearby homes were evacuated, and a cloud of acid fumes lingered over the site of the accident. One tanker car was carrying phosphoric acid, and another was carrying hydrochloric acid. Riverside County Fire captain said a one-mile radius had been set up around the accident site and no one was being let inside because of the potentially hazardous fumes.
   Source:
   http://www.cnn.com/2008/US/03/04/train.derail.ap/index.html?eref=rss_topstories

6. *March 4, Newsday* – (New York) **State seeks new plan to clean up chemical spill.** State health and environmental officials will be on hand to discuss a proposed plan to clean up chemical waste from Jimmy's Dry Cleaners in Roosevelt at a public meeting

scheduled for tomorrow night. Dry-cleaning solvents released during operations of the now-closed business have contaminated groundwater and soil vapor beneath the one-acre site and have also migrated about 3,400 feet south of the property, according to the state Department of Environmental Conservation. The DEC is also investigating whether vapor intrusion -- when volatile chemicals in groundwater vaporize and seep up through the ground into buildings -- is a concern over the contaminant plume. The DEC's proposed $4.7-million remedy would treat some of the highest concentrations of contaminants in the plume, but could result in untreated hazardous waste remaining at the site. The public comment period for the plan runs through March 12.
Source: http://www.newsday.com/news/local/nassau/ny-lidate045601169mar04,0,6359351.story

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

7. *March 4, York Daily Record* – (Pennsylvania) **Three Mile Island: In-house security.** The Three Mile Island nuclear station in Dauphin County, Pennsylvania, shifted Monday to an in-house security force, dubbed Exelon Nuclear Security. The transition is part of Exelon Nuclear's plans to replace Wackenhut Nuclear Services with an in-house security force at each of its ten generating stations. In November, Peach Bottom Atomic Power Station in Pennsylvania transitioned to Exelon Nuclear Security.
Source: http://www.yorkdailyrecord.com/ci_8443367?source=rss

8. *March 4, Associated Press* – (South Carolina) **Water leak at Oconee Nuclear Station reduces power levels.** A water leak on Monday at the Oconee Nuclear Station in South Carolina has cut power production to 73 percent, but plant officials say the leak has been fixed. A plant spokesman said that no radioactive material leaked and that the water leak was caught and corrected before any damage occurred. Power from other plants will make up for the reduced output and customers will not have any interruptions. The unit will continue to run at the reduced level until it is shut down for refueling and maintenance in April.
Source: http://www.wspa.com/midatlantic/spa/news.apx.-content-articles-SPA-2008-03-04-0002.html

9. *March 4, Reuters* – (Florida) **FPL Fla. Turkey Pt 3 reactor back at full power.** Florida Power & Light's nuclear Unit 3 at Turkey Point power plant exited an outage and ramped up to full power by early Tuesday, the U.S. Nuclear Regulatory Commission said. Both nuclear reactors and one natural gas unit at the plant shut on February 26 due to the loss of off-site power during south Florida's blackout.
Source:
http://www.reuters.com/article/rbssIndustryMaterialsUtilitiesNews/idUSN0445016320080304

[Return to top]

Defense Industrial Base Sector

10. *March 4, Appleton Post-Crescent* – (National) **Oshkosh Corp. unveils new vehicle.** Oshkosh Defense unveiled last week the first palletized load system vehicle dedicated to the recovery of heavy armored vehicles. The U.S. Army is already using a version of the model for off-road operations.
    Source:
    http://www.postcrescent.com/apps/pbcs.dll/article?AID=/20080304/APC03/803040509/1888

11. *March 4, BBC News* – (National) **U.S. airbase e-mails go to town web.** Confidential U.S. Air Force (USAF) e-mails have been mistakenly sent to a tourism website. The e-mails were meant to go to the U.S. airbase at RAF Mildenhall in Suffolk, England, via its website. But instead they went to a town tourism website which had a similar address. The USAF said it had sent out an e-mail advising contacts, family, and friends of airmen based at the site to use the correct address. A Mildenhall resident set up the website "mildenhall.com" in the late 1990s to promote the town. But by 2001 he was starting to get hundreds of e-mails meant for people at the airbase. He received information once about presidential flight plans and once about U.S. military procedures and tactics. He has now decided to take his website down to avoid getting these messages. A USAF spokesman said: "In 2004, The 100 Communication Squadron advised [the man] to block unrecognizable addresses from his domain and have an auto-reply sent reminding people of the official Mildenhall domain."
    Source: http://news.bbc.co.uk/1/hi/england/suffolk/7277392.stm

12. *March 3, Navy Times* – (National) **New ship designs promising but untested.** The Navy is betting a very large and expensive chunk of its future fleet on untested technologies and unprecedented practices: Large destroyers built to a hull design no one has ever ridden; aircraft carriers launching planes by a method yet to send a single aircraft aloft; littoral combat ships operated in ways new to any navy. The three projects have been in the works for years, but now the service is about to begin building the destroyers, construction has just begun on the first of the new carriers, and the first LCS will take to sea in a few months. That the Navy is depending on so many untried designs at once is epic. And these new ships do not represent modest leaps. To reduce risk, the Navy often has introduced new technologies in small steps. That step-by-step approach meant that teething problems with a new system did not hurt the entire design. And it provided a buffer in case a new technology failed. Today's Navy officials express confidence in their new ship programs, but worries persist that the destroyer's tumblehome hull design will be flawed, or that the carrier's revolutionary electromagnetic aircraft launch system will not be perfected before the ship is completed in 2015. "The introduction of several new classes within a limited span of years poses an acquisition management and supervision challenge for the Navy, and an execution challenge for industry," said a member of the Congressional Research Service.
    Source: http://www.navytimes.com/news/2008/03/navy_shiptech_030208/

[Return to top]

Banking and Finance Sector

13. *March 4, Chicago Sun-Times* – (National) **Buyer beware of tax prepares.** The Better Business Bureau says nearly a third of complaints it receives against tax preparation companies allege that the preparer made an error or mistake in the return that required the consumer to pay fines or added fees to rectify the problem. Disputes over billing accounted for 19 percent of the roughly 700 complaints the agency received from 2005 to 2007, and being unable to get a response from the preparer, including getting copies of their tax information or answers to questions, accounted for nearly 20 percent of complaints. Here is the BBB's advice on how to choose the right tax preparation company: Look for credentials. Ideally tax preparers should either be a certified public accountant, tax attorney or an enrolled agent; think access and choose one that is open year-round, in case you are audited; ask how much it costs for the service and how it will be affected if preparation is more complicated and time consuming. Also ask if the tax preparer will represent the consumer in the case of an audit; get referrals and check the Better Business Bureau Reliability Report on such services free of charge at *www.bbb.org*.
Source: http://www.suntimes.com/business/currency/823790,CST-FIN-wallet04WEB1.article

14. *March 4, Associated Press* – (South Carolina) **Bill would help residents avoid identity theft.** The Senate has approved a bill to allow South Carolina residents to freeze their credit to help protect them from identity theft. The bill says people can put a security freeze on their credit, which means no new loans or credit would be approved. Residents could temporarily unfreeze accounts for free when they want to open new accounts. South Carolina is among only ten states without an identity theft protection law. Only Indiana prevents credit companies from charging about $10 per freeze or temporary lift. The bill faces another vote this week in the House, which approved it last month. If the House agrees with the Senate's changes, it will go to the governor. The bill also requires companies and state agencies to notify customers when a security breach occurs.
Source: http://www.wistv.com/Global/story.asp?S=7957560&nav=menu36_22_7

15. *March 3, KUTV 2Utah* – (Utah) **Cell phone phishing scam.** At the Salt Lake Credit Union, the bank phone has been busy. Members and non-members alike are all calling in to find out about the same thing; bogus text messages received on cell phones all over Utah, sent by would-be thieves trying to steal their personal information. "I actually received one of these messages," says the vice president of the Salt Lake Credit Union. "This is a new thing to all of us with text messaging." The message says "your Salt Lake Credit Union bill service is expired," and it gives an 800 number to call and renew. "If you did get this message, don't respond," says the bank official. "If you have responded, contact us." When reports of the scam came in, the Credit Union jumped into action. Together with the F.B.I. and the Secret Service, they shut the number down. The Credit Union says they do not know who owned the number.
Source: http://www.kutv.com/content/gephardt/story.aspx?content_id=70665c51-39a9-4ed7-b549-512552e67497

[Return to top]

Transportation Sector

16. *March 4, Times-Picayune* – (National) **Ports act to improve security.** A partnership of five ports on the lower Mississippi River will begin developing a regional security program to deter terrorism between Plaquemines Parish and Baton Rouge. The Lower Mississippi River Port Wide Strategic Security Council said Monday that it has hired two companies to plan for a video surveillance system as well as a larger policy to guide future security efforts. Vanguard Technologies of Baton Rouge will prepare the video surveillance plan, and URS Corp. of San Francisco will undertake the strategic plan. The two documents should be complete by the end of August, said the council's executive director. "When the ports were working separately on the issue of security, it was more like we were in competition with each other for funds," said the executive director of the Port of South Louisiana. "A regional approach made much more sense." The Port of South Louisiana is the top tonnage port in the United States, moving 225.5 million tons of cargo in 2006, according to the American Association of Port Authorities. It is a grain hub and therefore critical to the world's food supply. Large quantities of other important products, such as crude oil and coal, also travel through the port. Four of the five ports represented by the council were among the nation's top 13 ports in 2006, moving a combined 414.6 million tons of cargo, according to the most recent statistics from the ports association.
Source: http://www.nola.com/business/t-p/index.ssf?/base/money-3/1204611673284920.xml&coll=1

17. *March 3, Associated Press* – (National) **Homeland Security warn states of airport hassles if they don't adopt ID rules.** Homeland Security officials are pushing recalcitrant states to adopt stricter driver's license standards to end a standoff that could disrupt domestic air travel. States have less than a month to send a letter to the Homeland Security Department seeking an extension to comply with the Real ID law passed following the 2001 terror attacks. Some states have resisted, saying it is costly, impractical and an invasion of privacy. Four states -- Maine, Montana, New Hampshire and South Carolina -- have yet to seek an extension. To bring the states in line, the Homeland Security secretary warned that any state that does not seek an extension by the end of March will find that, come May, their residents will not be able to use their licenses to board domestic flights. His assistant secretary sent letters to several governors Monday reminding them of the looming deadline, and urging the holdouts to seek an extension. If the states do not seek an extension by March 31, their residents will be subjected to secondary screening by security workers before boarding any domestic flight beginning May 11.
Source: http://www.foxnews.com/story/0,2933,334702,00.html

18. *March 3, Aero-News Network* – (National) **FAA oversight of foreign-sourced aircraft parts under scrutiny.** Boeing promises a serious review of a new report from the US Department of Transportations Office of the Inspector General (OIG), which claims poor FAA oversight of foreign manufacturers continues to allow substandard parts to find their way into US airliners. According to the Washington Post, the report was made public by the Project on Government Oversight, a nonprofit organization that focuses on

government accountability. The OIG charges the FAA's new records-review-based oversight model is missing problems which would be obvious if actual on-site inspections were conducted at foreign parts suppliers. "Neither manufacturers nor FAA inspectors have provided effective oversight of suppliers; this has allowed substandard parts to enter the aviation supply chain," reads the report, dated February 26. The OIG notes four engine failures in 2003, that were traced to "unapproved design changes made by a supplier" of engine fuel pump sensors. The report goes on to specifically mention concerns raised by Boeing's widespread international sourcing of parts and subassemblies for the upcoming 787 Dreamliner. The OIG states the FAA needs to immediately review its own procedures and guidelines, and make the necessary changes. Downplaying the ominous undertones of the OIG report, the FAA stressed "there are absolutely no imminent safety issues raised by the report," according to an agency spokeswoman. Given the report's potential impact to its most highly-anticipated new aircraft program, Boeing took particular interest in the OIG's findings. The report notes of 17 major structures on the Dreamliner, 13 are to be produced at least in part by overseas companies.
Source: http://www.aero-news.net/index.cfm?ContentBlockID=b28889dd-5ba1-452e-a209-f3339ae3ca74

[Return to top]

Postal and Shipping Sector

Nothing to Report

[Return to top]

Agriculture and Food Sector

19. *March 4, USAgNet* – (National) **USDA rejects 'downer' cow ban.** The secretary of Agriculture told Congress last week that he would not endorse an outright ban on "downer" cows entering the food supply or back stiffer penalties for regulatory violations by meat-processing plants in the wake of the largest beef recall in the nation's history. Appearing at a Senate Appropriations subcommittee hearing, he said the U.S. Department of Agriculture is investigating why it missed the inhumane treatment of cattle at the Westland/Hallmark Meat Co. in Chino, California, including workers administering electric shocks and high-intensity water sprays to downer cows – those too sick or weak to stand without assistance. The secretary announced interim steps such as more random inspections of slaughterhouses and more frequent unannounced audits of the nearly two dozen plants that process meat for federal school lunch programs.
Source: http://www.wisconsinagconnection.com/story-national.php?Id=535&yr=2008

20. *March 4, WLNS 6 Lansing* – (National) **Meijer recalling frozen dinners.** The Grand Rapids, Michigan-based retailer Meijer has issued a recall on over 2,000 pounds of frozen entrees in four states, including Michigan. The recall includes 12-ounce packages of Discover Cuisine red curry chicken and jasmine rice. They are labeled with a Canadian establishment number of 302 on the front and a use-by date of December 18,

2008. The products are being recalled because of possible listeria contamination. No illnesses have been reported.
Source: http://www.wlns.com/Global/story.asp?S=7961461&nav=0RbQ

21. *March 3, Reuters* – (International) **Japan snafu won't slow talks to boost beef trade-USDA.** A 20-ton beef shipment to Japan that mistakenly contained extra boxes of meat intended for distribution in the United States will not slow efforts by the Agriculture Department to fully reopen trade with its one-time largest customer, a USDA spokesman said on Monday. The beef shipment included an additional 25 boxes that had not been ordered, but were being held in the same Arizona facility. The plant, operated by Smithfield Foods Inc. has been temporarily banned from shipping beef to Japan. Beef shipments from the United States were banned by Japan soon after the first case of mad cow disease was found in Washington in December 2003. Trade resumed in the summer of 2006, but Japan has suspended shipments from plants that have shipped beef cargoes that violate the bilateral agreement or are without required documentation. U.S. officials had hoped a decision last May by the World Organization for Animal Health, which gave the United States a "controlled risk" status for beef safety, would boost beef exports significantly, but there has been little change. After the decision, the United States expected South Korea, Japan, China, and other markets to relax import restrictions for U.S. beef. U.S. officials have encouraged trading partners to adopt international beef guidelines by accepting U.S. bone-in beef and meats from cattle of all ages.
Source:
http://www.reuters.com/article/companyNews/idUSN0337832520080303?sp=true

[Return to top]

Water Sector

22. *March 4, Los Angeles Times* – (California) **L.A. County, Malibu accused of violating clean-water rules.** Conservation groups on Monday sued Los Angeles County and the city of Malibu to force them to clean up the slurry of fecal bacteria, copper, lead, cyanide, and other pollutants being washed down storm drains, creeks, and rivers into coastal waters. The two lawsuits, filed in U.S. District Court in Los Angeles, are test cases aimed at enforcing compliance with Clean Water Act rules first adopted 17 years ago. The cases rely on annual reports filed by the county showing that it violates limits set for bacteria, heavy metals, and other pollutants carried by rainfall or sprinkler runoff down the Los Angeles and San Gabriel rivers, Ballona and Malibu creeks, and other discharge points into Southern California waters. Up to this point, these so-called storm water rules required county and city officials to take steps toward cleanup, such as mounting education campaigns and stenciling storm drains with no-dumping warnings explaining that the channels flow into the ocean. The lawsuit does not specify how the county and city should meet the standards of the Clean Water Act. Those details would be left to government officials. Southern California has long had one of the nation's worst urban runoff problems, largely because so much of the landscape has been paved over or developed. All of this hardened landscape tilts toward the sea; so most of the rain in the area rushes into coastal waters, sweeping contaminants along with it. This

pollution, according to various studies, contributes to gastrointestinal illnesses among Southern California beachgoers, increases the toxicity of fish caught in local waters, and spurs harmful algae blooms that can poison marine life.
Source: http://www.latimes.com/news/printedition/california/la-me-drain4mar04,1,5573220.story

23. *March 4, Times* – (Indiana) **Contamination found in Michigan City creek.** A forgotten underground tank is being blamed for contamination that was found flowing into Trail Creek in Michigan City, Indiana. The contamination was discovered about 3 p.m. Sunday by four men who were fishing. They noticed a sheen on the water and an odor a conservation officer described as similar to paint thinner or old gasoline. The men reported their find to the Indiana Department of Natural Resources Law Enforcement Division. Officers traced the problem to an underground tank at the Blocksom Co., which is located on the creek. The tank apparently was unused for decades, eventually filled with water and began overflowing. The Indiana Department of Environmental Management took samples to determine the nature of the pollution and arranged for a company that handles hazardous materials to pump the contaminated liquid from the tank. Blocksom will be responsible for removing the tank and any contaminated soil from the surrounding area.
Source:
http://www.thetimesonline.com/articles/2008/03/04/news/porter_county/doc5b9db6deff8ead1586257402001e3d5a.txt

24. *March 2, Miami Herald* – (Florida) **Water treatment plant is designed to do double duty.** Hallandale Beach moved into the 21st century recently with a new water treatment plant that is also ready to serve as a regional emergency operations center. Hurricanes, saltwater intrusion, the increasing cost of delivering more drinkable water into homes and businesses, even the threat of terrorism, are addressed inside the building. The facility, in combination with the city's still-operational outdoor water treatment system just yards away, pumps out about seven million gallons of water a day. Constructed to withstand Category 5 hurricane force winds, the building surrounds an elaborate "membrane system" made up of dozens of cylindrical modules that push about three and a half million gallons of water a day from the county's well field through 72 monitoring points. The offices that overlook the two-story indoor membrane system are used by public works administration and engineering staff. If disaster strikes, the place is equipped to convert in two hours to a regional emergency command post. "We have everything we need – generators that will run for months, computers, televisions, communications systems, windows with shutters that can withstand 200 mph wind," the city manager said.
Source: http://www.miamiherald.com/472/story/438322.html

[Return to top]

Public Health and Healthcare Sector

25. *March 3, in-Pharma Technologist* – (International; National) **Supply chain globalization weighs heavily on FDA.** The globalization of the supply chain

increasingly challenges the U.S. Food and Drug Administration's ability to ensure the quality of pharmaceuticals on the U.S. market, acknowledges the acting director of the agency's Center for Drug Evaluation and Research. Addressing a hearing of the House Agriculture, Rural Development, the Food and Drug Administration. and Related Agencies Appropriations Subcommittee last week, the FDA's chief medical officer and deputy commissioner for scientific and medical programs noted that the agency now routinely reviews and monitors drugs – from both innovator and generic companies – that are "studied or manufactured, at least in part, outside the United States." This changing environment, which included "the fundamental challenges of many different languages and protocols," meant the agency had to "devise and evaluate more complex risk scenarios and apply more sophisticated technologies to screen and evaluate drugs entering the United States to ensure their quality," she said. She warned that the growth in the FDA's capacity to inspect generic drug manufacturing facilities "has not been commensurate with this global expansion."
Source:
http://www.in-pharmatechnologist.com/news/ng.asp?n=83656-fda-cder-inspection-pharmaceutical-manufacturing-import

26. *March 3, KGTV 10 San Diego* – (California) **TB warning in effect for local clinic.** An unidentified individual associated with a blood plasma collection center in downtown San Diego contracted tuberculosis, prompting county health officials Monday to warn clients and staff who may have been exposed. A spokeswoman for the San Diego County Health and Human Services Agency (HHSA), declined to say whether the person was an employee or a patient at Life Sera Plasma Collection Center. According to the HHSA, the individual was at the center from last July 1 to February 18, and officials have identified staffers and hundreds of clients that were potentially exposed to the disease.
Source: http://www.10news.com/health/15478287/detail.html

27. *March 3, Associated Press* – (Nevada) **Hepatitis C in Nev. could be 'tip of iceberg.'** An outbreak of hepatitis C at a Nevada clinic may represent "the tip of an iceberg" of safety problems at clinics around the country, according to the head of the Centers for Disease Control and Prevention. The city of Las Vegas shut down the Endoscopy Center of Southern Nevada last Friday after state health officials determined that six patients had contracted hepatitis C because of unsafe practices, including clinic staff reusing syringes and vials. Nevada health officials are trying to contact about 40,000 patients who received anesthesia by injection at the clinic between March 2004 and January 11 of this year to urge them to get tested for hepatitis C, hepatitis B, and HIV. "This is the largest number of patients that have ever been contacted for a blood exposure in a health care setting. But unfortunately we have seen other large-scale situations where similar practices have led to patient exposures," the head of the CDC said.
Source: http://www.usatoday.com/news/nation/2008-03-03-hepatitis-nevada_N.htm?csp=15

Government Facilities Sector

28. *March 4, CNN* – (Mississippi) **Reported tornado tears through National Guard barracks.** A possible tornado touched down late Monday in southern Mississippi, slashing through a National Guard barracks and injuring 14 guardsmen, according to a sheriff and a military spokesman. The barracks housed guardsmen from Mena, Arkansas, who are training at Shelby. Camp Shelby is a Joint Forces Training Center about 75 miles northwest of Mobile, Alabama.
    Source: http://www.freerepublic.com/focus/f-news/1980128/posts

29. *March 3, KGW 8 Portland* – (Oregon) **Multiple agencies respond to anthrax scare.** In Oregon, an early morning anthrax scare at the Linn County Court House turned out to be a hoax. The Federal Bureau of Investigation, the Department of Homeland Security, and the Linn-Benton Hazmat Team all responded to the call. Around 6:15 a.m. a custodian found a note on an outside door indicating envelopes containing anthrax were inside and outside the courthouse. One person was in the building when the note was discovered. The Linn County Sheriff closed the courthouse while hazmat teams searched for anthrax. Only two envelopes connected to the note were found. One was slid under a door. The other was left with the note outside. Neither contained anthrax.
    Source: http://www.kgw.com/news-local/stories/kgw_030308_local_anthrax_linn_county.1e277278.html

30. *March 3, WJAC 6 Johnstown* – (Pennsylvania) **Bomb threat forces courthouse evacuation again.** A bomb threat put trials on hold again Monday morning at the Blair County, Pennsylvania, courthouse. The call came into the 911 center just before 8 a.m. County officials said although they were able to resume business as usual, it is no less troubling. Two threats forced officials to close the courthouse in Hollidaysburg for a day in January, which resulted in a loss of time and thousands of dollars for the county. When the Blair County 911 center received the call Monday morning, employees evacuated again so police could sweep the building inside and out. There have been no arrests so far in relation to the January bomb threat. However, a major drug trial was going on that day and another drug trial was on Monday's agenda. County officials said, as they continue to work with law enforcement to track down the people responsible, they will be looking for a possible link between the drug trials and the threats.
    Source: http://www.wjactv.com/news/15480949/detail.html

31. *March 3, Boston Globe* – (Rhode Island) **Bomb threat evacuates large building at URI.** Up to 700 people were evacuated from a building at the University of Rhode Island (URI) after a report of a bomb threat, a school spokeswoman said. Authorities began searching the building at 12:50 p.m. There have not been any reports of an actual bomb being found. University police received a call just after noon from a person who had overheard a conversation about a bomb threat at Independence Hall, said a URI spokeswoman. About 700 students were scheduled to be in the three-story academic building at the time.
    Source:
    http://www.boston.com/news/local/breaking_news/2008/03/bomb_threat_eva.html

32. *March 3, Hawaii Reporter* – (Illinois) **Muslim woman arrested for terrorist threat against University of Illinois.** A 24-year-old Wheaton, Illinois, resident was arrested for making e-mail threats against the University of Illinois-Chicago campus. The suspect was charged in a criminal complaint filed in federal court in Chicago with one count of making threats through use of interstate commerce, which is a felony offense. According to the police complaint, an individual subsequently identified as the suspect, who is a student at the university, sent an anonymous e-mail to a university administrator threatening a repeat of the shooting incident that had taken place the previous day at Northern Illinois University. The threat stated that a group of five individuals would carry out the attack sometime during the spring 2008 semester. However, the caller failed to give a reason for making the threat.
    Source: http://www.hawaiireporter.com/story.aspx?b455d857-dc30-4fc5-acf6-bc0d51a71d53

[Return to top]

Emergency Services Sector

33. *March 3, 2008, Government Technology* – (Washington) **Seattle opens new state-of-the-art emergency operations center.** On the eve of the seventh anniversary of the Nisqually earthquake, Seattle's mayor opened a new state-of-the-art Emergency Operations Center (EOC), a high-tech nerve center that will coordinate the city's response to disasters and other major events. The new EOC is a critical step forward in fulfilling the mayor's goal of making Seattle the most prepared city in the country for dealing with emergencies, whether natural or human caused. It is the latest project delivered by the 2003 Fire Levy. "We can't stop the next earthquake or storm from striking Seattle, but we can be prepared to save lives, protect property and pull ourselves up after a disaster," the mayor said. The new EOC has state-of-the-art technology and space to better allow the city to coordinate emergency responses and keep the public informed. It is designed to withstand major earthquakes, with a seismic standard 50 percent higher than most buildings. The new EOC will allow the city to coordinate with regional, state, and national operations centers through a host of systems and back-up systems, including the Internet, video-teleconferencing, satellite phones, 800 MHZ radio, short-wave/amateur radio, and local, state, and national warning/notification radios.
    Source: http://www.govtech.com/gt/268765?topic=117691

[Return to top]

Information Technology

34. *March 4, Los Angeles Times* – (International) **China's computer hacking worries Pentagon.** China in the last year has developed ways to infiltrate and manipulate computer networks around the world in what U.S. defense officials conclude is a new and potentially dangerous military capability, according to a Pentagon report issued Monday. Computer network intrusions at the Pentagon and other U.S. agencies, think

tanks, and government contractors last year "appeared to originate" in China, according to the report. In addition, computer intrusions in Germany, apparently by Chinese hackers, occur daily, along with infiltrations in France and Britain, the Pentagon said. The Pentagon report does not directly accuse the Chinese military or government of the attacks but says the incidents are consistent with recent military thinking in that country. A U.S. deputy assistant secretary said cyber-warfare was an area of growing concern, and he called on the Chinese to clarify their intentions.
Source: http://www.1913intel.com/2008/03/04/chinas-computer-hacking-worries-pentagon/

35. *March 4, TechWorld* – (International) **Criminals automate security testing.** Cybercriminals are starting to resemble the legitimate software industry to such an extent that they even pre-test malware applications for effectiveness before rolling them out. That is according to PandaLabs, which has found forums on which criminals hook up with one another to push ahead with development of applications which can be used to test their creations against known security products. In a blog, the company analyses several of the malware-testing applications it has found to be in use recently, including the particularly effective KIMS, Scanlix, and Multi-AVs Fixer. Either tool can tell a malware author whether their application would be detected by one or more of a large range of anti-virus products. The main disadvantage of these is that they require a full copy of the security programs to be present locally, an onerous task given that this means having 15 or more programs installed at any one time in order to cover the field. Testing a malevolent application against security products is useful for any malware author, mainly because even quite crude applications have to attempt to disable security to have any chance of working. But carrying out testing application-by-application is bound to be hugely time-consuming. "Even if their creations were detected by one or two companies, they could still launch them, as they would affect all users with different security technologies," said a PandaLabs representative.
Source: http://www.networkworld.com/news/2008/030308-criminals-automate-security.html

36. *March 3, Network World* – (National) **Identity management critical for security, government IT shops say.** A majority of government IT organizations say identity management is very important to securing their networks and will become even more so over the next five years, but that funding to keep pace is a major impediment to growth. The respondents also said they think identity management is relevant to national security, critical public infrastructure, and personal security; and, given the gravity of those issues, that personal privacy could suffer. The findings were part of a survey of 474 government IT professionals conducted by public-opinion research firm Pursuant, and funded by Quest Software. A majority of the respondents were civilians working for the federal government and not in the U.S. Department of Defense, according to Quest. Slightly more than 33 percent of the respondents said increased physical, data and information security was the top reason for building an identity-management system. Compliance with such government mandates as HSPD-12 – which lays out a policy for a common identification standard for federal employees and contractors – was the No. 2

reason at 32.1 percent. Protection of personal information (19 percent), and simplified internal data systems (2.5 percent) were the third and fourth reasons. The respondents said identity management was critical because they feared data breaches could have devastating consequences, including loss of personal privacy and data security, compromised critical public infrastructure, deflated national security, and increased financial terrorism.
Source: http://www.networkworld.com/news/2008/030308-identity-management-critical-for-security.html

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: http://www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Communications Sector

37. *March 3, Computer Weekly* – (International) **Counterfeit Cisco gear threatens network security.** The seizure of £38m worth of counterfeit Cisco equipment has raised concerns over the security of networks. Last week the US Department of Justice and Department of Homeland Security seized more than 400 counterfeit Cisco network hardware and labels. The equipment included counterfeit network hardware, in particular network routers, switches, network cards and modules manufactured by Cisco. Penetration testing specialist SecureTest warned that government and communications networks could be infected with malicious firmware imported from places in the Far East, such as China. Unlike current malware, machine level hardware such as the chipsets used in routers and switches and other computer devices are rarely tested and may already have established back doors in communications systems across the country, the company said. Users looking to buy Cisco gear have very little guidance as to how to spot fake Cisco equipment, as any attempt at publishing guidance would simply alert the counterfeiters -- who would then be able to correct the differences between their products and the genuine article. In one message board a network administrator suggested people simply look at the price. “There are a lot of ways to spot fake Cisco, with a too good to be true low price being the very first one. However, it is too dangerous to ‘publicly disclose’ this information as the counterfeiters will use it to ‘correct’ their mistakes.” The problem for network administrators is that the counterfeit network equipment is very good and so it can be difficult to spot differences. UsedCisco.com has produced a guide that recommends, among other things, that users avoid buying used Cisco gear from eBay and direct from China, and that they check holograms and make sure documentation is written in English, using the same font and without spelling mistakes. In addition, serial numbers should be checked against Cisco’s database.
Source: http://www.computerweekly.com/Articles/2008/03/04/229675/counterfeit-

cisco-gear-threatens-network-security.htm

[Return to top]

Commercial Facilities Sector

38. *March 3, Associated Press* – (National) **OSHA to inspect plants like Ga. refinery.** Federal inspections will be carried out at hundreds of plants where combustible dust is a workplace hazard, a top safety official said Monday at a sugar refinery where dust is suspected of causing a deadly explosion. The head of the Occupational Safety and Health Administration (OSHA) announced the inspections while visiting the Imperial Sugar refinery in Port Wentworth, where a blast on February 7 killed 12 workers and injured dozens more. OSHA has not completed its investigation of that explosion but is sending letters to 30,000 companies that deal with combustible dust to discuss the dangers, the official said in a telephone interview. Combustible dust standards were put in effect for the grain industry after a series of explosion in the 1980s, but OSHA declined to act on a 2006 recommendation by the U.S. Chemical Safety Board that similar standards be set up for other industries. Last month, the United Food and Commercial Workers International Union and the International Brotherhood of Teamsters petitioned OSHA to take that step. The official said Monday that more work must be done to determine whether existing standards on ventilation and factory housekeeping can be used to address existing concerns, and to determine how a standard can be crafted so it makes sense for different industries with different types of dust. Source: http://www.usatoday.com/news/nation/2008-03-03-osha-inspections_N.htm?csp=15

[Return to top]

National Monuments & Icons Sector

Nothing to Report

[Return to top]

Dams Sector

Nothing to Report

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-5389
Removal from Distribution List:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-5389 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us–cert.gov or visit their Web page at www.us–cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.